Department of Homeland Security Daily Open Source Infrastructure Report for 16 March 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- Dow Jones reports officials are trying to follow a paper trail of ownership, sales, and other records to confirm a cow that contracted bovine spongiform encephalopathy was born before the U.S. enacted cattle−feed safety rules in 1997. (See item 18)
- The Associated Press reports Iowa state health officials say they are concerned about a rare strain of mumps −− the genotype G strain infrequently seen in the U.S. −− behind an outbreak of 60 cases in Iowa. (See item 23)
- The Associated Press reports an 1890s−era Hawaiian plantation dam failed in the rugged hills above northern Kauai, sending water and mud surging through two homes and wiping out the only highway. (See item 40)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *March 15, Los Angeles Times* — **Natural gas terminal off California coast is proposed.** Australia's Woodside Energy, hoping to overcome environmental and safety concerns, unveiled plans on Wednesday, March 15, to place a liquefied natural gas terminal in the Pacific Ocean about 22 miles south of Malibu. This is the latest of half a dozen proposals to meet California's

growing demand for clean−burning energy by importing liquefied natural gas. A debate over the safest way to handle the volatile fuel has plaqued all of the projects. Under Woodside's proposal, the gas would be pumped from Australian fields, super cooled to a liquid and transported in specially designed tanker ships. Upon arrival at the offshore terminal, the liquid would be turned back into a gas while still aboard ship, and then sent via underwater and overland pipelines to the Southern California Gas Co. delivery network. The terminal, which would be little more than a ship mooring with a flexible connection to the pipeline, involves no permanent structure that can be seen from shore, said Jane Cutler, president of Woodside's Los Angeles−based subsidiary. Cutler said the proposed site was close to the giant Los Angeles market and was also the best of 17 locations studied between Monterey Bay and the Camp Pendleton Marine base.
Source: http://www.latimes.com/business/la−fi−lng15mar15,1,1802724.story?coll=la−headlines−business

2. *March 14, Government Accountability Office* — **GAO−06−531T: Managing Sensitive Information: DOE and DoD Could Improve Their Policies and Oversight (Testimony).** In the interest of national security and personal privacy and for other reasons, federal agencies place dissemination restrictions on information that is unclassified yet still sensitive. The Department of Energy (DOE) and the Department of Defense (DoD) have both issued policy guidance on how and when to protect sensitive information. DOE marks documents with this information as Official Use Only (OUO) while DoD uses the designation For Official Use Only (FOUO). GAO was asked to (1) identify and assess the policies, procedures, and criteria DOE and DoD employ to manage OUO and FOUO information; and (2) determine the extent to which DOE's and DoD's training and oversight programs assure that information is identified, marked, and protected according to established criteria. In its report issued earlier this month, the Government Accountability Office (GAO) made several recommendations for DOE and DoD to clarify their policies to assure the consistent application of OUO and FOUO designations and increase the level of management oversight in their use. DOE and DoD agreed with most of GAO's recommendations, but partially disagreed with its recommendation to periodically review OUO or FOUO information. DoD also disagreed that personnel designating a document as FOUO should mark it with the applicable FOIA exemption.
Highlights: http://www.gao.gov/highlights/d06531thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−531T

3. *March 07, Government Accountability Office* — **GAO−06−369: Managing Sensitive Information: Departments of Energy and Defense Policies and Oversight Could Be Improved (Report).** In the interest of national security and personal privacy and for other reasons, federal agencies place dissemination restrictions on information that is unclassified yet still sensitive. The Department of Energy (DOE) and the Department of Defense (DoD) have both issued policy guidance on how and when to protect sensitive information. DOE marks documents with this information as Official Use Only (OUO) while DoD uses the designation For Official Use Only (FOUO). The Government Accountability Office (GAO) was asked to (1) identify and assess the policies, procedures, and criteria DOE and DoD employ to manage OUO and FOUO information and (2) determine the extent to which DOE's and DoD's training and oversight programs assure that information is identified, marked, and protected according to established criteria. GAO made several recommendations for DOE and DoD to clarify their policies to assure the consistent application of OUO and FOUO designations and increase the

level of management oversight in their use. DOE and DoD agreed with most of GAO's recommendations, but partially disagreed with its recommendation to periodically review OUO or FOUO information. DoD also disagreed that personnel designating a document as FOUO should also mark it with the applicable FOIA exemption.
Highlights: http://www.gao.gov/highlights/d06369high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−369

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *March 15, Sun Journal (ME)* — **Propane leak prompts business closure.** A small propane leak forced businesses in Sabattus, ME, to temporally close Tuesday night, March 14, until the Sabattus Fire and Police departments were able to pinpoint the problem. Fire Chief Don Therrien described the problem as a small propane leak coming from the cap of a tank belonging to Yeung's Chinese Restaurant.
Source: http://www.sunjournal.com/news/city/20060315072.php

[Return to top]

Defense Industrial Base Sector

5. *March 15, Government Accountability Office* — **GAO−06−356: Joint Strike Fighter: DoD Plans to Enter Production before Testing Demonstrates Acceptable Performance (Report).** The Joint Strike Fighter (JSF) is the Department of Defense's (DoD) most expensive aircraft program. The program represents 90 percent of the remaining planned investment for recapitalizing DoD's aging tactical aircraft fleet. The Government Accountability Office (GAO) is required by law to review the program annually for 5 years, beginning in fiscal year 2005. This is our second report and GAO assessed the program's acquisition approach −− in terms of capturing knowledge for key investment decisions −− and identified an alternative to improve outcomes. The Congress should consider delaying authorizations and appropriations for JSF procurement until a new business case is developed and flight testing demonstrates the design and integrated mission systems work. GAO included this matter for consideration because DoD did not plan to make changes as a result of recommendations. GAO is recommending that DoD delay investing in production until flight testing shows that the JSF performs as expected, and that the program develop a plan, consistent with DoD's preferred policy, to adopt an evolutionary approach that limits new content for each increment to proven technologies and design. DoD partially concurred, but believes that its current practices achieve our recommendations' objectives.
Highlights: http://www.gao.gov/highlights/d06356high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−356

6. *March 15, Government Accountability Office* — **GAO−06−447: Unmanned Aerial Systems: New DoD Programs Can Learn from Past Efforts to Craft Better and Less Risky Acquisition Strategies (Report).** Through 2011, the Department of Defense (DoD) plans to spend $20 billion to significantly increase its inventory of unmanned aircraft systems, which

are providing new intelligence, surveillance, reconnaissance, and strike capabilities to U.S. combat forces −− including those in Iraq and Afghanistan. Despite their success on the battlefield, DoD's unmanned aircraft programs have experienced cost and schedule overruns and performance shortfalls. Given the sizable planned investment in these systems, the Government Accountability Office (GAO) was asked to review DoD's three largest unmanned aircraft programs in terms of cost. Specifically, GAO assessed the Global Hawk and Predator programs' acquisition strategies and identified lessons from these two programs that can be applied to the Joint Unmanned Combat Air Systems (J−UCAS) program, the next generation of unmanned aircraft. GAO recommends that DoD (1) limit Global Hawk production until the program demonstrates an integrated system and develops a new business case to justify future investments and (2) develop a sound business case and acquisition strategy for J−UCAS and follow−on efforts to ensure cost and schedule goals are met. DoD did not concur with our Global Hawk recommendations because it believes it is taking appropriate measures to manage risk.
Highlights: http://www.gao.gov/highlights/d06447high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−447

7. *March 15, Government Accountability Office* — **GAO−06−327: Defense Acquisitions: Initial Missile Defense Capability Shows Knowledge−Based Acquisition Strategy Is Needed (Report).** The Department of Defense (DoD) has spent nearly $90 billion since 1985 to develop a Ballistic Missile Defense System. In the next six years, the Missile Defense Agency (MDA), the developer, plans to invest about $58 billion more. MDA's overall goal is to produce a system that is capable of defeating enemy missiles launched from any range during any phase of their flight. MDA's approach is to field new capabilities in 2−year blocks. The first −− Block 2004 −− was to provide some protection by December 2005 against attacks out of North Korea and the Middle East. This year's report assesses (1) MDA's progress during fiscal year 2005 and (2) whether capabilities fielded under Block 2004 met goals. To the extent goals were not met, the Government Accountability Office (GAO) identifies reasons for shortfalls and discusses corrective actions that should be taken. To better ensure the success of future development efforts, GAO recommends that MDA implement a knowledge−based acquisition strategy for future missile defense efforts, assess whether such a strategy is compatible with a 2−year block strategy, and adopt more transparent criteria for reporting significant departures from plans. DoD did not agree to take any of the actions we recommended.
Highlights: http://www.gao.gov/highlights/d06327high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−327

8. *March 14, Government Accountability Office* — **GAO−06−367: Defense Acquisitions: Improved Business Case Needed for Future Combat System's Successful Outcome (Report).** The Department of Defense (DoD) anticipates that the Future Combat System (FCS) will modernize the U.S. Army's ability to move, shoot, and communicate on the battlefield. It is an impressive concept that is the product of holistic, non−traditional thinking. The Army describes FCS as one of the most complex weapon acquisition programs ever executed because it involves developing and integrating a family of 18 systems and an information network. Army leadership started the program early as part of its effort to change Army culture and believes that the program risks are manageable. The Government Accountability Office (GAO) is required by law to review the program annually. In this report, GAO analyzes FCS's acquisition business case and assesses requirements stability, technology maturity, soundness of

the acquisition strategy, reasonableness and affordability of program costs. In order to improve the FCS's business case, GAO is making recommendations to the Secretary of Defense that involve setting clear expectations for progress and evaluating that progress by 2008. DoD partially concurred with our recommendations. This report also contains matters for congressional consideration to ensure FCS has a sound business case before future funding commitments are made.
Highlights: http://www.gao.gov/highlights/d06367high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−367

9. *March 14, Government Accountability Office* — **GAO−06−364: Joint Strike Fighter: Management of the Technology Transfer Process (Report).** The Joint Strike Fighter (JSF) program is the Department of Defense's (DoD) largest international cooperative effort to develop and produce a major weapon system. Due to the breadth of international participation, the number of export authorizations needed to share information with partner governments, solicit bids from suppliers, and execute contracts is expected to far exceed past transfers of advanced military technology. In July 2003, the Government Accountability Office (GAO) reported that managing these transfers and partner expectations while avoiding delays has been a key challenge and recommended that industrial planning tools be developed and used to anticipate time frames for national disclosure and technology transfer decisions. This report examines DoD's response to this recommendation and identifies the practices DoD is using to expedite license processing and avoid program delays.
Highlights: http://www.gao.gov/highlights/d06364high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−364

10. *March 14, Government Accountability Office* — **GAO−06−449: Space Acquisitions: DoD Needs a Departmentwide Strategy for Pursuing Low−Cost Responsive Tactical Space Capabilities (Report).** For more than two decades, the Department of Defense (DoD) has invested heavily in space assets to provide the warfighter with mission−critical information. Despite these investments, DoD commanders have reported shortfalls in space capabilities. To provide tactical capabilities to the warfighter sooner, DoD recently began developing TacSats −− a series of small satellites intended to be built within a limited time frame and budget −− and pursuing options for small, low−cost vehicles for launching small satellites. The Government Accountability Office (GAO) was asked to (1) examine the outcomes to date of DoD's TacSat and small, low−cost launch vehicle efforts, (2) identify the challenges in pursuing these efforts, and (3) determine whether experiences with these efforts could inform DoD's major space system acquisitions. GAO is recommending that DoD assign accountability for developing and implementing a departmentwide strategy for pursuing low−cost tactical capabilities −− both satellite and launch vehicles −− and identify corresponding funding. In commenting on the report, DoD agreed with the recommendation.
Highlights: http://www.gao.gov/highlights/d06449high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−449

[Return to top]

Banking and Finance Sector

11.

March 14, Tech Web — **Americans want banks to spy on their accounts.** Nine out of ten Americans want their banks to monitor their online accounts for signs of suspicious behavior, such as credit card companies do now, a survey published Tuesday, March 14, said. Conducted by RSA Security, the poll also found that although consumers aren't seeing a rise in the number of phishing e−mails, they are increasingly wary of all electronic communiqués from their banks. A solid majority of 59 percent want their banks to contact them when something fishy is found, while 73 percent think banks should boost security by moving to a stronger authentication scheme than the typical username and password.
RSA Press Release: http://www.rsasecurity.com/press_release.asp?doc_id=6636&id= 1034
Source: http://www.techweb.com/wire/security/181503554;jsessionid=CAD4T12HABT0AQSNDBCSKHSCJUMEKJVN

12. *March 13, Tech Web* — **Free CipherTrust toolbar pegs phishing, spots spam.** Security vendor CipherTrust on Monday, March 13, released a free toolbar for Microsoft Outlook and Lotus Notes that graphically displays the likelihood that individual messages are spam or phishing attacks. The toolbar offers recommendations on the legitimacy of each message that hits an Outlook or Notes inbox, said CipherTrust.
CipherTrust's toolbar: http://research.ciphertrust.com/tools.php?tool=toolbar
Source: http://www.techweb.com/wire/security/181503214;jsessionid=RBCNMHUOKYNJQQSNDBCSKHSCJUMEKJVN

[Return to top]

Transportation and Border Security Sector

13. *March 15, Associated Press* — **US Airways to recall 400 flight attendants.** US Airways Group will recall up to 400 furloughed flight attendants based on seniority as it prepares to ramp up its schedule for the busy summer travel season. The airline is the nation's fifth largest, created with the September combination of US Airways and America West Airlines. The new airline is run primarily by former America West executives, and is based in Tempe, AZ. US Airways was in bankruptcy protection at the time of the combination and had a large number of employees on furlough status. As of March 1, approximately 1,600 flight attendants, 1,500 pilots and 4,400 other employees were still furloughed. The company recently recalled 55 furloughed pilots and announced plans to hire 200 new reservation agents this year.
Source: http://www.usatoday.com/travel/flights/2006−03−15−usair−atte ndants_x.htm

14. *March 15, Associated Press* — **FAA: Planned 39−story hotel could pose risk to planes at Sky Harbor.** The Federal Aviation Administration (FAA) has made a preliminary determination that a planned 39−story luxury hotel and condominium project in downtown Phoenix could be an obstruction because of its proposed 450−foot height. The FAA does not have the authority to stop the project. But officials determined that the hotel's height could pose a hazard to aircraft and pilots using nearby Sky Harbor International Airport. Phoenix officials and the development team on Tuesday, March 14, downplayed the significance of the FAA's findings, saying they were optimistic that the $200 million−plus project would ultimately get a favorable ruling. City officials believe the project will ultimately go forward because they have recently completed an analysis of all buildings in the downtown area and altered the proposed height limits for the airspace around portions of Sky Harbor.

Source: http://www.usatoday.com/travel/hotels/2006−03−15−hotel−skyha rbor_x.htm

15. *March 15, Associated Press* — **Train with sulfuric acid derails in Illinois.** A train hauling sulfuric acid overturned early Wednesday, March 15, forcing the evacuation of about 250 southern Illinois homes in a half−mile radius of the accident, authorities said. Emergency crews were determining whether any of the 92,000 pounds of sulfuric acid it was carrying had leaked, said David Searby, operations officer for Du Quoin Emergency Services. The chemical can burn skin and trigger asthma attacks.
Source: http://www.boston.com/news/nation/articles/2006/03/15/train_with_sulfuric_acid_derails_in_ill/

16. *March 15, SecureIDNews* — **E−Passport trial will conclude at San Francisco airport.** The 90−day San Francisco trial is scheduled to conclude on April 15, 2006. The Department of Homeland Security is overseeing the tests. According to its spokesperson, Kimberly Weissman, they are testing the security feature known as Basic Access Control (BAC), a process designed to help prevent the unauthorized reading, or skimming, of information from e−Passports. Basically, the machine−readable zone (MRZ) of the passport is scanned and a key is created based on its contents. This key is then used to authenticate the passport before any of the passport holder's information is transmitted. Using BAC, no personal information can be transmitted via the contactless interface unless the passport has been purposefully opened and its MRZ read and authenticated. “We’re working with Australia and New Zealand because (some) citizens have already been issued the passports,” said Weissman. So far, about 70,000 passports have been issued to New Zealand citizens, along with airline crews from Singapore.
Source: http://www.secureidnews.com/library/2006/03/15/epassport−trial−underway−at−san−francisco−airport/

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

17. *March 15, Xinhua (China)* — **Japan confirms 23rd mad cow case.** A 68−month−old diary cow on a farm in northern Japan's Hokkaido was confirmed to have contracted mad cow disease, the Japanese Ministry of Health, Labor and Welfare announced Wednesday, March 15. This is Japan's 23rd case of mad cow disease, or bovine spongiform encephalopathy. According to the ministry's statement, the cow, which was raised in Nakagawa, Hokkaido prefecture, was suspected to have caught the disease in a preliminary test on Monday, March 13. Its sample was later sent for re−examination and the results were also positive.
Source: http://news.xinhuanet.com/english/2006−03/15/content_4307236 .htm

18. *March 14, Dow Jones* — **U.S. Department of Agriculture following paper trail to get age of bovine spongiform encephalopathy infected cow.** U.S. officials are trying to follow a paper

trail of ownership, sales, and other records to confirm a cow that contracted bovine spongiform encephalopathy (BSE) was born before the U.S. enacted cattle−feed safety rules in 1997. The U.S. Department of Agriculture (USDA) confirmed the latest BSE case on Monday, March 13, saying the cow had spent about a year on an Alabama farm. A preliminary age estimate of 10 years old was made based on a dental exam performed by a veterinarian in Alabama, where the cow was found. USDA officials have said they believe contaminated feed is the way in which two previous BSE−infected cows found in the U.S. contracted the disease. Jay Truitt, with the National Cattlemen's Beef Association, said that because the infected cow was likely at least 10 years old, following a paper trail will be much harder than if the animal were younger. If the cow went through livestock markets, Truitt said, records might be just sheets of paper stapled to copies of sales receipts. Another possibility, he said, would be a record of a brucellosis vaccination. Such a record, if it exists, may be a three−by−five card in the file cabinet of a veterinarian.
Source: http://www.cattlenetwork.com/content.asp?contentid=23105

19. *March 14, Daily Sentinel (CO)* — **With chronic wasting disease rates static, practice of culling deer and elk will stop.** With statewide infection rates of chronic wasting disease (CWD) in big game not showing much change a half−decade after the Colorado Division of Wildlife (DOW) began killing infected deer and elk, the practice will stop. The infection rate of deer continues to be anywhere from less than one percent up to 10 percent of the local populations, with the heaviest infections on the Front Range in what's known as the endemic area. Elk show markedly lower signs of infection, from less than one to about 2.6 percent of the local population. Most of the CWD occurring in elk is found in the northwestern quarter of the state. Mike Miller, state veterinarian for the DOW, said the culling programs showed "no clear evidence of any kind of beneficial affect" on CWD control.
CWD information: http://www.cwd−info.org/
Source: http://www.gjsentinel.com/sports/content/sports/stories/2006/03/14/3_15_OUT_CWD_culling_held_WWW.html

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

20. *March 14, Associated Press* — **Drought forces suspension of some water rights.** Dry conditions have forced South Dakota to issue shutoff orders to 54 irrigators on the Cheyenne River and tributaries upstream of Angostura Reservoir near Hot Springs. The U.S. Bureau of Reclamation has a more senior water right −− dating to 1941 −− that allows the reservoir to fill to provide irrigation water to the Angostura Irrigation District, according to the state Department of Environment and Natural Resources. Because Angostura is less than half full, the Bureau of Reclamation asked that state permits for other water uses be suspended so all available water flows into the reservoir. It is the third straight year that drought−related shutoff

orders were issued. They apply to irrigation, municipal uses, or commercial uses but not to domestic uses such as livestock watering.
Source: http://www.aberdeennews.com/mld/aberdeennews/news/14099035.h tm

21. *March 13, Los Angeles Times* — **Drought threat seen in Europe.** The drought that looms over much of western and southern Europe this summer is already creating problems in Britain, France, and Spain. Winter rainfall has been disappointing across much of the continent. With some countries still recovering from the effects of a relatively dry winter last year and the heat wave of 2003, sustained heavy rain over the next two months would be needed to avoid the risk of drought this summer. In Britain, the government warned of lawn watering bans in the southern counties. The French government has launched a campaign to urge farmers and the public to use water sparingly. Corn growers are being asked to consider the viability of their thirsty crop. Electricity generation could become problematic if the drought persists, as nuclear power stations, which provide three−quarters of French electricity, need to be able to take large amounts of water from rivers. If water is scarce or too warm, the power plants can face shutdown. In Spain, which officials say is suffering its most serious drought in more than a century, the government is to announce an emergency plan for the worst affected areas in the south and center of the country.
Source: http://www.latimes.com/business/la−ft−drought13mar13,1,4101205.story?coll=la−headlines−business

[Return to top]

Public Health Sector

22. *March 15, Associated Press* — **Bird flu hits Sweden; Afghans suspect it.** Sweden recorded its first case of the H5N1 bird flu strain on Wednesday, March 15, saying European laboratory tests confirm two wild birds found dead in the southeast were infected with the virus. Afghan authorities, meanwhile, said preliminary test results from a United Nations lab left them "99 percent certain" that the country's first bird flu outbreak was the H5N1 strain. Danish authorities said they too had found a wild bird infected with an aggressive strain of bird flu, but it was not immediately whether it was the H5N1 strain. If confirmed as H5N1, it would be the first case of the virus in Denmark. Also Wednesday, March 15, Myanmar announced it had culled 5,000 poultry to prevent the spread of bird flu, as authorities in western India prepared to slaughter tens of thousands of chickens.
Source: http://abcnews.go.com/Health/wireStory?id=1727563

23. *March 15, Associated Press* — **Iowa officials concerned about mumps cases.** State health officials said they are concerned about a rare strain of virus behind an outbreak of 60 mumps cases in Iowa. Mary Gilchrist, director of the state's University Hygienic Laboratory, said the genotype G strain is infrequently seen in the U.S. With the number jumping from 17 cases just two weeks ago, she predicted there could be more outbreaks this spring. So far, there are 18 cases recorded in Johnson County, 16 in Dubuque, five in Black Hawk County, and four in Scott County. Two cases were confirmed in Linn County, while other counties have one to three cases. The patients with confirmed cases of mumps range in age from 11 to 41, but Gilchrist said half have been college students. She said the virus may have come from Europe, but a similar strain has been detected in New Jersey. The U.S. Centers for Disease Control and

Prevention is investigating the source.
Mumps information: http://www.cdc.gov/nip/diseases/mumps/default.htm
Source: http://www.cbsnews.com/stories/2006/03/15/ap/health/mainD8GB N0FO0.shtml

24. *March 14, Japan Times* — **System targets bioterror, flu threats.** The Infectious Disease Surveillance Center at the National Institute of Infectious Diseases in Tokyo, Japan, is working on the surveillance system so that prompt countermeasures can be taken to prevent the spread of infections. Under the planned system, the center will continuously collect and analyze data of people seeking medical attention and determine that an abnormal situation has arisen in the event there are 10 or more patients in a certain region complaining of symptoms such as fever, convulsions or vomiting. It will then dispatch a medical team to the affected region for diagnoses, decontamination and to prevent the spread of infection.
Source: http://search.japantimes.co.jp/cgi−bin/nn20060314a8.html

25. *March 14, Agence France−Presse* — **Fever grips Madagascar as doctors uncertain of cause.** Since early January, nearly all the residents of Madagascar's eastern port town of Toamasina have been struck by a fever, a symptom doctors have failed to attribute with certainty to either disease currently affecting the coastal population. The medics suspect dengue fever or a crippling mosquito−borne disease called chikungunya, but they cannot exactly tell the cause as both illnesses have near identical symptoms, are spread by the same vector and have no known cure nor vaccine. "In the last three months, between 80 and 90 percent of Toamasina residents have had a fever," said Clarette Dinh−Van, a general physician operating a private clinic in Toamasina, home to some 200,000 people and Madagascar's largest port. Early this month, health officials said the island had recorded its first cases of chikungunya, which is attributed to the deaths of some 93 people in the French overseas territory of Reunion. They also announced cases of dengue fever. The Indian Ocean island lacks medical facilities to carry out proper diagnosis. Since last month about 20 blood samples were taken to France for analysis.
Chikungunya information: http://www.phac−aspc.gc.ca/msds−ftss/msds172e.html
Dengue fever information: http://www.cdc.gov/ncidod/dvbid/dengue/index.htm
Source: http://news.yahoo.com/s/afp/20060314/hl_afp/healthmadagascar disease_060314165535;_ylt=AkkSiRMBm1EHnKgnQ2A..MmJOrgF;_ylu= X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

26. *March 13, European Space Agency* — **Researchers convinced satellites are helpful in tracking epidemics.** The amount of data acquired by satellites is increasing at an exponential rate, and researchers are learning about the value of this data in fighting epidemic outbreaks as a result of European Space Agency's (EPA) Epidemio project. The Epidemio project was developed in January 2004 to illustrate the benefits of remote−sensing data for studying, monitoring, and predicting epidemic outbreaks. By using data which focuses on a region's landscape −– rainfall, vegetation, water bodies, elevation, dust mapping, and temperature −– researchers are able to pinpoint climatic conditions which are favorable for harboring various epidemic hosts, indicating where people are at greatest risk. Ghislain Moussavou of the International Center for Medical Research began studying Ebola fever in Congo and Gabon in the hope of spotting particular environmental characteristics associated with infected sites. Combining ESA Envisat satellite data, under the Epidemio project, on water bodies, forest cover, and digital elevation models with field results, Moussavou and his team were able to link

the epidemic with dryness and drought. The Epidemio project concludes its two−year mission in April 2006.
Source: http://www.esa.int/esaCP/SEM5FINVGJE_index_0.html

[Return to top]

Government Sector

27. *March 15, Government Accountability Office* — **GAO−06−528T: Capitol Visitor Center: Status of Project Schedule and Costs as of March 15, 2006 (Testimony).** Since the Subcommittee's February 15 Capitol Visitor Center (CVC) hearing, the CVC team has continued to move the project's construction forward, but we continue to believe, as we said at the February hearing, that the Architect of the Capitol's (AOC) proposed opening dates −− April 2007 for the base CVC project and May 2007 for the House and Senate expansion spaces −− do not allow enough time to complete several critical activities and to address problems, challenges, risks, and uncertainties. During the past month, the CVC team has essentially maintained the pace of critical interior wall stone installation, developed a draft work plan for floor stone installation, started to develop a work plan to prevent a stacking of trades during finish work, and maintained the opening dates that AOC announced at the February CVC hearing. If the CVC team is successful in addressing these issues, we believe that the base CVC project can be opened to the public with a temporary cap on visitor occupancy in May 2007 and that the expansion spaces can be opened for occupancy beginning in mid−August to early September 2007.
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−528T

[Return to top]

Emergency Services Sector

28. *March 15, Sun−Herald (FL)* — **Annual Tactical Search and Rescue Drill conducted in Florida.** Sarasota County, FL, conducted its annual Tactical Search and Rescue Drill Tuesday, March 14, in North Port. The drill, named "Operation North Port 2006," involved teams from North Port, Sarasota County, Venice and Sarasota. The drill involved multiple obstacles where participants needed to render emergency life support, transportation of victims and prisoners, neutralize downed power lines, and maintain security within the team's operations, said Richard Berman, operations chief of Sarasota County's Emergency Management. Berman said the drill was designed to present terrorist scenarios, including: downed poles; a police car accident with downed wires, a gas leak, and two patients, one a police officer and the other a prisoner; medical emergencies; someone putting a bomb together in a house; a K−9 search; and a waste spill involving people covered with waste. The objectives North Port did well on were: maintain communications in the field through the deployment and utilization of assets; ability to investigate and analyze and disseminate ongoing information to protect the public safety; integrating various assets to establish and maintain scene safety and to test equipment, assets and skills of first responders.
Source: http://www.sun−herald.com/NewsArchive2/031506/np1.htm?date=031506&story=np1.htm

29. *March 14, KSDK (MO)* — **Missouri holds tornado drills, but not everyone hears sirens.** Three days after deadly tornadoes blasted through the area, Missouri emergency officials put the tornado warning system to the test. Cities such as Festus, Hillsboro and Arnold are equipped with sirens. But in the nearby Jefferson R−7 school district, there are no sirens. Educators rely on radios and the fire department to keep them informed. In fact, officials say 75 percent of the 660−square−miles of Jefferson County are not covered by sirens. Presiding Commissioner Mark Merkens says there are no current plans to create a siren system.
Source: http://www.ksdk.com/news/news_article.aspx?storyid=93672

30. *March 13, Homeland Response (OH)* — **Chicago: Preparing for disaster.** Many of Chicago's emergency response preparations require residents to be aware and involved of their own safety. Since the 9/11 attacks, Chicago has taken a number of steps to protect the city's residents and infrastructure, including participating in one of the largest disaster drills ever launched in the United States. Unlike the residents of many large U.S. cities, those in Chicago have a pretty good idea of how the city and its responders will handle a major disaster. The city's emergency systems were tested in the TOPOFF 2 mock terrorism exercise in May 2002. City officials agreed that valuable lessons were learned: the importance of communication systems and warning systems; proper training and equipment for first responders; and surveillance of public areas. In January 2006, the city launched a new disaster preparedness campaign, Alert Chicago, which focuses on public awareness. Alert Chicago is designed to provide simple and easy−to−follow instructions on how communities can prepare for emergencies, as well as how they should respond to various disaster scenarios. In addition, the city has implemented an emergency Telephone Notification System that can call every phone in an area of the city at the rate of 1,000 calls per minute.
Alert Chicago Website: http://webapps.cityofchicago.org/ChicagoAlertWeb/
Source: http://www.homelandresponse.org/500/Issue/Article/False/1360 6/Issue

31. *March 13, USCD News (CA)* — **Calit2 researchers deploy disaster communications network at San Diego Mardi Gras festivities.** Last month, a team of nearly 30 researchers from the California Institute for Telecommunications and Information Technology (Calit2) joined forces with San Diego law enforcement to make sure San Diegans and out−of−town visitors had a safe Mardi Gras on February 28. The researchers built a wireless network made up of high−tech gadgets, including a satellite dish, cameras, wireless network boxes, laptops and even cell phones. Then they gave law enforcement access to the network and data it produced, such as video feeds. The project’s goal is to develop technologies that enable public safety officials and first responders to gather, use and disseminate information during an emergency. The Mardi Gras drill allowed researchers to test drive a wireless system that could be used in disasters and emergencies. Police and first responders said they were impressed with the technologies Calit2 provided. San Diego Police Chief William Lansdowne urged his lieutenants to work with the researchers to make some of the innovations available for the use of emergency officials in the event that a real disaster strikes.
Source: http://ucsdnews.ucsd.edu/thisweek/2006/mar/03_13_mardigras.a sp

[Return to top]

Information Technology and Telecommunications Sector

32. *March 15, Security Focus* — **IBM Tivoli Lightweight Client Framework information disclosure vulnerability.** Tivoli Lightweight Client Framework (LCF) is prone to an information disclosure vulnerability. Analysis: The HTTP interface of Tivoli LCF allows an authenticated user to have read access to files with root authority by manipulating the configuration of log files. Vulnerable: IBM Tivoli Lightweight Client Framework 3.7.1.
Solution: The vendor has released an advisory along with configuration parameters to resolve this issue. For further detail:
http://www−1.ibm.com/support/docview.wss?rs=0&q1=vulnerability+OR+vulnerabilities&uid=swg21082896&loc=en_US&cs=utf−8&cc= us&lang=en
Source: http://www.securityfocus.com/bid/17085/references

33. *March 15, Security Tracker* — **Adobe Graphics Server interactive login configuration lets remote users execute arbitrary code.** A vulnerability was reported in Adobe Graphics Server. A remote user can cause arbitrary code to be executed on the target system. Analysis: When configured according to vendor recommendations, a remote user may be able to cause arbitrary code to be executed on the target system. The remote user can load arbitrary code onto the server such that it will be executed the next time an interactive user login occurs. The code will run with the privileges of the Adobe Server service account. On some systems, this may be system level privileges. Only Windows based systems are affected. Vulnerable versions: Version(s): 2.0, 2.1.
Solution: The vendor recommends following a manual hardening process as well as restricting interactive logins to the service account for the server (adbeserv) by using local security policies. The vendor's advisory describes the service account restriction steps and is available at: http://www.adobe.com/support/techdocs/332989.html
Source: http://securitytracker.com/alerts/2006/Mar/1015769.html

34. *March 15, Secunia* — **Flash Player unspecified code execution vulnerabilities.** Some vulnerabilities have been reported in Flash Player, which can be exploited by to compromise a user's system. Analysis: The vulnerabilities are caused due to unspecified errors and can be exploited to execute arbitrary code on a user's system when a malicious SWF file is loaded. Affected software: Macromedia Breeze 4.x; Macromedia Breeze 5.x; Macromedia Breeze Meeting Add−In; Macromedia Flash 8.x; Macromedia Flash MX 2004; Macromedia Flash MX Professional 2004; Macromedia Flash Player 7.x; Macromedia Flash Player 8.x; Macromedia Flex 1.x; Shockwave Player 10.x.
Solution: Install updated versions.
Flash Player 8.0.22.0 and earlier: Update to version 8.0.24.0 or 7.0.63.0.
http://www.macromedia.com/go/getflash
Flash Player 8.0.22.0 and earlier −− network distribution: Update to version 8.0.24.0 or 7.0.63.0. http://www.macromedia.com/licensing/distribution
Flash Professional 8, Flash Basic: Update to version 8.0.24.0.
http://www.macromedia.com/support/flash/downloads.html
Flash MX 2004: Update to version 7.0.63.0.
http://www.macromedia.com/support/flash/downloads.html
Flex 1.5: Update to version 8.0.24.0. http://www.macromedia.com/go/3d2855d6
Breeze Meeting Add−In: Update to version 7.0.55.331 (Win) or 7.0.55.118 (Mac).
http://adobe.breezecentral.com/common/help/en/support/downlo ads.htm

Shockwave Player: Update to version 10.1.1.
http://www.macromedia.com/shockwave/download/
Source: http://secunia.com/advisories/19218/

35. *March 15, New York Times* — **Study says chips in ID tags are vulnerable to viruses.** A group of European computer researchers have demonstrated that it is possible to insert a software virus into radio frequency identification tags (RFIDs), part of a microchip−based tracking technology in growing use in commercial and security applications. In a paper entitled, "Is Your Cat Infected With a Computer Virus?," to be presented Wednesday, March 15, at an academic computing conference in Pisa, Italy, the researchers plan to demonstrate how it is possible to infect a tiny portion of memory in the chip, which can hold as little as 128 characters of information. Until now, most computer security experts have discounted the possibility of using RFID chips to spread a computer virus because of the tiny amount of memory on the chips. Ultimately, by their research, they have introduced a series of worrisome prospects, including the ability of terrorists and smugglers to evade airport luggage scanning systems that will use RFID tags in the future.
Source: http://www.nytimes.com/2006/03/15/technology/15tag.html?ex=1300078800&en=24f421ff24864376&ei=5090&partner=rssuserland&em_c=rss

36. *March 15, Government Computer News* — **NIST sets FISMA standards for federal IT systems.** The National Institute of Standards and Technology (NIST) has released the final standard for securing agency computer systems under the Federal Information Security Management Act (FISMA). Federal Information Processing Standard 200 sets minimum−security requirements for federal systems in 17 security areas. It is the third of three publications required from NIST under FISMA, which requires executive branch agencies to establish consistent, manageable IT security programs for non−national security systems. The intent of FISMA is to implement risk−based processes for selecting and implementing security controls.
Source: http://www.gcn.com/online/vol1_no1/40127−1.html

37. *March 14, Government Accountability Office* — **GAO−06−526T: Telecommunications: Options for and Barriers to Spectrum Reform (Testimony).** The radio−frequency spectrum is used to provide an array of wireless communications services that are critical to the U.S. economy and various government missions, such as national security. With demand for spectrum exploding, and most useable spectrum allocated to existing users, there is growing concern that the current spectrum management framework might not be able to respond adequately to future demands. This testimony, which is based on previous Government Accountability Office (GAO) reports, provides information on (1) the extent to which the Federal Communications Commission (FCC) has adopted market−based mechanisms for commercial use, (2) the extent to which market−based mechanisms have been adopted for federal government users of spectrum, (3) options for improving spectrum management, and (4) potential barriers to spectrum reform. In previous reports, GAO recommended that (1) the Secretary of Commerce and FCC should jointly develop a national spectrum plan to guide decision making, and (2) the relevant administrative agencies and congressional committees work together to develop and implement a plan for the establishment of an independent commission that would conduct a comprehensive examination of current spectrum management. To date, these recommendations have not been implemented.

Highlights: http://www.gao.gov/highlights/d06526thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−526T

38. *March 14, U.S. Computer Emergency Readiness Team* — **US−CERT Technical Cyber Security Alert TA06−073A: Microsoft Office and Excel Vulnerabilities.** Microsoft has released updates that address critical vulnerabilities in Microsoft Office and Excel. Exploitation of these vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code or cause a denial−of−service on a vulnerable system. Systems affected: Microsoft Office for Windows and Mac OS X; Microsoft Excel for Windows and Mac OS X; Microsoft Works Suite for Windows.
Solution: Apply updates: Microsoft has provided the updates for these vulnerabilities in the Security Bulletins and on the Microsoft Update site.
Security Bulletins: http://www.microsoft.com/technet/security/bulletin/ms06−mar. mspx
Microsoft Update site: https://update.microsoft.com/microsoftupdate/v6/muoptdefault.aspx?ln=en&returnurl=https://update.microsoft.com/microsoftupdate/v6/default.aspx?ln=en−us
Workarounds: Please see the following US−CERT Vulnerability Notes for workarounds:
http://www.kb.cert.org/vuls/byid?searchview&query=VU%23682820,VU%23339878,VU%23104302,VU%23123222,VU%23235774,VU%2364242 8
Source: http://www.uscert.gov/cas/techalerts/TA06−073A.html

39. *March 13, Computer World* — **McAfee antivirus update wreaks havoc.** A faulty antivirus update from McAfee Inc. that mistakenly identified hundreds of programs as a Windows virus has resulted in some companies accidentally deleting significant amounts of data from affected computers. The McAfee update (DAT 4715) released on Friday, March 10, was designed to protect computers against the W95/CTX virus. But because of a programming error, the update also incorrectly identified, renamed and quarantined hundreds of legitimate executables. For companies that had configured their McAfee antivirus program to automatically delete bad files, the error resulted in the loss of hundreds, and in some cases even thousands, of files on systems in which the update had been installed, said Johannes Ullrich, chief technology officer at the SANS Internet Storm Center in Bethesda, MD. McAfee released a new patch (DAT 4716) updating the earlier one, five hours later.
Source: http://www.computerworld.com/securitytopics/security/story/0,10801,109525,00.html?SKC=security−109525

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT reports publicly that Apple Security Update 2006−001 resolves a number of vulnerabilities affecting Mac OS X, OS X Server, Safari web browser, and other products. Please review the following

vulnerability Notes:

VU#999708 − Apple Safari automatically executes arbitrary shell commands or code Apple Safari fails to properly determine file safety, allowing a remote unauthenticated attacker to execute arbitrary commands or code. http://www.kb.cert.org/vuls/id/999708

VU#351217 − Apple Safari WebKit component vulnerable to buffer overflow Apple Safari WebKit component is vulnerable to buffer overflow. This vulnerability may allow are remote attacker to execute arbitrary code or cause a denial of service condition. http://www.kb.cert.org/vuls/id/351217

VU#176732 − Apple Safari vulnerable to buffer overflow Apple Safari is vulnerable to a stack based buffer overflow. This vulnerability may allow a remote attacker to execute arbitrary code on a vulnerable system. http://www.kb.cert.org/vuls/id/176732

Apple has provided Security Update 2006−001 that addresses additional vulnerabilities not described above. http://docs.info.apple.com/article.html?artnum=303382

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 80 (www), 25 (smtp), 445 (microsoft−ds), 139 (netbios−ssn), 12106 (−−−), 2234 (directplay), 32459 (−−−), 32774 (sometimes−rpc11) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

40. *March 15, Associated Press* — **One dead, seven missing after dam in Hawaii breaks.** An 1890s−era plantation dam failed in the rugged hills above northern Kauai, sending water and mud surging through two homes and wiping out the only highway. Searchers found one person dead and were looking for at least seven others, some of them children who hadn't been seen since the deluge. The continuing rain was hampering the search and road−clearing efforts, and officials were worried that other old earthen dams in the area may have been catastrophically weakened by days of heavy rain, state Senator Gary Hooser said. Governor Linda Lingle, who planned to tour the area Wednesday, March 15, extended state disaster programs and services to the residents affected by recent rains and flooding. State officials were assessing the safety of other dams in the island's steep hills. Ed Teixeira, state vice director of civil defense, said officials were worried about erosion. Nearly all of Hawaii's dams were built early in the past century before federal standards existed or the advent of the state's program for assessing dam and levee safety, according to Edwin Matsuda, an engineer who heads the state's safety programs.

Source: http://www.usatoday.com/news/nation/2006−03−14−hawaii−dam_x. htm

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer